

Remarks

I. Status of Claims

Without prejudice, the claims have been amended to address a number of informalities. First, a number of informalities have been corrected in accordance with the examiner instructions. Specifically, Claim 1 has been amended to recite “verifying said receive certificate...,” Claim 2 has been amended to eliminate “said trust entity certificates,” Claim 15 has been revised to recite “said signing certificate”, and the second instance of Claim 52 has been changed to Claim 53 and the subsequent claims have been renumbered 54-56 respectively. Additionally, new claims 57-61 have been added. Support for these claims can be found in withdrawn Claim 9, ¶0071, ¶0061, ¶0061, and ¶0021, respectively.

II. Claim Rejections – 35 U.S.C. §112

The Examiner rejected Claims 2 and 53 under 35 U.S.C. §112 because the term “said trust entity certificates” lacks antecedent basis, and because there are two instances of Claim 52. Without prejudice, the claims have been amended as described above to obviate these rejections.

III. Prior Art Rejections

The Examiner rejected Claims 1, 22, 24 and 29-30 under 35 U.S.C. §102(b) as being anticipated by Micali (U.S. Patent No. 5,717,757). Specifically, the Examiner states as follows:

Micali discloses downloading a trust information object (TIO) wherein the TIO comprises at least a plurality of hash values, each hash value being hashed from a trust entity certificate, and a plurality of trust factors each trust factor corresponding to a hash value and being indicative of the level of trust associated with a particular entity certificate.

In making this rejection, the Examiner interprets the “CIL” disclosed by Micali as being a “TIO”. The Examiner states further as follows:

Micali discloses that a certificate authority (CA) creates the CIL. An intermediary receives the CIL and can further forward the CIL to others. The CIL itself is disclosed in many embodiments. In one embodiment, it could contain a plurality of hash values obtained by hashing certificates and also containing information related to the validity of the certificates which the Examiner is interpreting as trust vectors.

With respect to the second step, the Examiner states as follows:

An intermediary could be sent an entire certificate to verify the status of the certificate (i.e., its trust vector). Micali discloses that one way to verify the certificate is to hash a certificate and compare the hash value to a hash value on hand, (i.e., stored in the CIL). Information regarding the status of the certificate (i.e., if it is issued, revoked, valid, etc.) is sent back to the user who sent the certificate to the intermediary for verification.

Alternatively, the Examiner rejects Claims 1, 22, 24, 29-30 50-54 and 56 under 35 U.S.C. §103(a) as being unpatentable over Hericourt¹ in view of Samar² (U.S. Patent No. 6,304,974) in view of Micali (U.S. Patent No. 5,717,757). With respect to Claims 1 and 22, the Examiner states:

The Examiner is interpreting the CAS table as seen in device 308 (see Figure 3) as a TIO. The table contains a plurality of records related to CAF certificates. As discussed in paragraphs 11 and 17 a certificate could contain such information as a hash value or a certificate itself. Note that Hericourt does not place any limit on the type of certificates that could be used in his invention. As seen in Figure 5, each record in the table contains the certificate itself, thus the CAF table contains a plurality of hash values hashed from the CA certificate since each certificate contains its own hash. Each record also contains a CA-trust-level 507, which the Examiner is interpreting as a trust vector. Because there are multiple records there is a plurality of trust vectors in the CAF table, each vector corresponding to the certificate in the hash value. Hericourt also discloses verifying a received certificate (paragraph 104).

¹ Applicants do not agree that Hericourt is prior art as its effective date is after the priority filing date of present application. Nevertheless, applicants choose to distinguish the claimed invention over Hericourt based on its merits, rather than having it removed as a reference.

² Applicants do not agree that Samar is necessarily prior art because applicants may have made their invention prior to Samar's effective date. Nevertheless, at this time, applicants choose to distinguish the claimed invention over Samar based on its merits, rather than having it removed as a reference.

The Examiner admits that Hericourt does not expressly disclose downloading a trust information object (TIO) from a server to the memory of the client. The Examiner states, however, that “since Hericourt does not explicitly explain how the administrator maintains the table, one of ordinary skill would recognize that Hericourt’s invention is one which is ready for improvement and one in which one of ordinary skill could apply a variety of known table maintenance techniques to achieve the table maintenance.” The Examiner goes on to state that “Samar discloses one manner in which the table is provided to a client is by downloading the table to the client by an administrator (column 8, lines 20-39).” The Examiner concludes “it would have been obvious to incorporate Samar’s teaching with the Hericourt invention because “one would do so by having Hericourt’s security administrator create a CF table and download the table from the administrators computer (i.e., a server) to a device 0308’s memory, i.e., a clients memory.” The Examiner states the rationale for doing so is that Hericourt’s invention is “ready for improvement.”

The Examiner also admits that Hericourt does not explicitly disclose verifying a receive certificate by hashing said receive certificate to generate a resulting hash value as claimed. The Examiner states, however, that the limitation is disclosed by Micali. The Examiner states “that one would have been motivated to verify a certificate according to Micali’s teachings because as recognized by Micali, hashes produce fewer bits, thus comparison for purposes of verification would be faster via use of hashes rather than comparing the entire certificate.”

In reply, Applicants respectfully submit that the claims are patentability distinct over Micali or the combination of Micali, Hericourt, and Samar.

A. Micali fails to disclose transmitting a TIO to a client

Contrary to the Examiner’s characterization, Micali does not anticipate the claimed invention. It is well established in US patent law that a reference anticipates a claim only if it discloses all the elements of the claim. Here, Micali does not disclose the TIO of the claimed invention. The TIO is an important aspect of the claimed invention and comprises hash values of various certificates, and a plurality of trust

vectors, each trust vector corresponding to a hash value and being indicative of the level of trust associated with a particular certificate. The trust vectors indicate, for example, the operations for which each certificate is trusted or is trusted to delegate to other certificates. Thus, the TIO correlates a hashed certificate with that certificate's authority level. This is an important feature of the claimed invention as it provides the client with the means to determine certificate authenticity with a relatively small file (for example, less than 1k as opposed to a conventional directory, which is 100-400k, see ¶¶ 0006 and 0071)

On the other hand, the CIL of Micali is merely a list of "issued" certificates and is intended to *supplement* a directory of certificates and a certificate revocation list (CRL). More specifically, the CIL was introduced to supplement a conventional certificate directory to avoid the problem of verifying certificates that are neither issued nor revoked. As set forth in Micali:

A user of an electronic communication system may query an intermediary (such as a Directory) with certificate identification information and obtain in response the identified certificate. Certificate identification information may be a serial number, a user name, a CA, etc.

...

The above procedure could present a problem if a user queries the Directory with a serial number that does not correspond to a certificate issued by the CA. In that case, the Directory, though possessing the relative certificate, may deny the user that information. Having the Directory provide the user with the latest CRL of the CA does not solve the problem either. In fact, the absence of the queried serial number from the CRL only proves that the corresponding certificate, if any, is not revoked, but leaves open the possibility that no certificate corresponding to the requested serial number (and CA) was ever issued. Since intermediaries may not be trusted, this is a problem, and may cause serious denial of service complications or attacks.

(Co. 5, ll. 63-col. 6, l. 18.) Therefore, Micali recognizes that conventional certificate verification processes, involving a user querying an untrusted intermediary having a certificate directory and a CRL, have a problem when the inquiry relates to a certificate which is neither issued nor revoked.

Micali purports to solve this problem by providing the CIL which is a listing of issued and/or non-issued certificates. As set forth in Micali:

The problem of a user querying an intermediary with certificate identifying information that does not correspond to any issued certificate may be addressed by means of a new structure, called a Certificate Issue List (CIL). A CIL may include a (preferably) dated and authenticated (e.g., digitally signed) list of all the serial numbers of issued (and preferably not expired) certificates. A CIL allows a (possibly) untrusted intermediary to prove whether a given certificate has been issued. A CIL may also contain additional information. For instance, the CIL may contain the issue date for each issued certificate and/or the issue date of the CIL.

(col. 8, ll. 31-42.) Therefore, Micali provides the CIL as a means for an untrusted intermediary to prove if a given certificate is issued/not issued. This way, the untrusted intermediary supplements the certificate directory with not only the CRL, but also now the CIL, to provide the user with an indication of the trustworthiness of a given certificate.

The CIL in this context is different from the TIO of the claimed invention. As claimed, the TIO comprises at least a plurality of hash values, each hash value being hashed from a trusted entity certificate, and a plurality of trust vectors, each trust vector corresponding to a hash value and being indicative of the level of trust associated with a particular trusted entity certificate. The TIO is provided to the client so the client is able to perform its authentication based on the TIO. Although Micali does indicate that a certificate identifier may be a hashed value of the certificate, nowhere does Micali indicate that these certificates are correlated with a requisite level of trust to establish a connection with the client.

The Examiner's interpretation that the issuance or non-issuance of a certificate is the same as its level of trust to establish a connection is not realistic. Specifically, it is not reasonable to equate the mere fact that a certificate is issued as in a CIL with a vector that indicates the operations for which the certificate is trusted or is trusted to delegate. In other words, the CIL provides information only about the existence of an issued certificate, while the TIO provides information about the quality of the

certificate. This is a major difference which cannot be ignored. Accordingly, because Micali does not anticipate the claimed invention, the rejection should be withdrawn and the claims allowed.

B. Micali fails to disclose verifying a received certificate by determining if its hashed value corresponds to one in the TIO and, if so, whether the corresponding trust vector is sufficient

Micali fails not only to disclose a TIO as claimed, but also to verify the received certificate based on the TIO and the trust vectors it contains. Specifically, as mentioned above, the claimed invention is directed to a server-based trust information delivery scheme in which the server provides the client with a relatively-small TIO to perform certificate verification. This verification involves hashing a received certificate, comparing the hashed value to the TIO, and, if a match is found, determining if the associated trust vector is sufficient for the intended operation. This is a critical aspect of the claimed invention and is not found in Micali.

Micali is devoid of an operation in which the TIO (or the CIL based on the examiner's interpretation) is queried for the level of trust of the certificate. This is not surprising since the CIL was never intended to provide this information. To the contrary, the CIL is *supplemental* to a directory of certificates and a CRL in a conventional certificate management scheme. In other words, as mentioned above, the CIL is used to plug a perceived deficiency in the conventional scheme, and is not intended to supplant the convention verification scheme as the TIO does in the claimed invention. Accordingly, the rejection should be withdrawn and the claims allowed.

C. The examiner's combination of Hericourt, Samar, and Micali fails to render the claimed invention obvious because the combination ignores the prior art as a whole

The examiner's rejection combines various teaching but fails to consider the prior art as a whole. It is well established in US patent law that the prior art must be considered as a whole, including aspects which teach away from the invention. By way of review, Hericourt is based on a traditional server-maintained certificate directory as described in the previous reply. Samar is a technique for ensuring the

authenticity of a downloaded directory by downloading the directory to a client using one communication path, and then downloading a thumbprint of the directory to the client using a different path. If the directory and its thumbprint correspond, then the client is assured that the directory is authentic. And finally, Micali, as described above, provides for a supplemental file, a CIL, which is downloaded to a user to prove which certificates are issued and which are not. Micali also indicates that the CIL may be in a reduced form, i.e., hashed certificates. The Examiner combines these teachings by starting with the Hericourt directory, modifying this directory to contain hashed certificates according to Micali, and then downloading it according to Samar.

The Examiner fails, however, to consider the art as a whole including those portions that teach away from this combination and modification. For example, the examiner ignores the fact that, in each reference, certificate verification is performed by referencing a conventional directory. Specifically, as admitted by the examiner, Hericourt does not disclose a TIO, and thus cannot rely on hashed certificates for verification. Likewise, Samar verifies certificates using a full-blown directory, and not a TIO having hashed certificates. The hashed directory in Samar is used only as verification of the conventional directory. Finally, as mentioned above, Micali does not use the CIL exclusively to authenticate certificates, but rather uses it in conjunction with a convention directory.

Therefore, since all of the references continue to rely on a conventional director to verify certificates, they remain fundamentally different from the claim invention which relies on a TIO. It is impermissible for the examiner to pick and choose certain features of the references to render the claimed invention obvious without acknowledging that each of the references relies on the very thing the claimed invention is aimed at eliminating—a relatively large, conventional, certificate directory. Accordingly, the rejection should be withdrawn and the claims allowed.

U.S. Patent Application No. 10/057,066
Attorney Docket No. TVW/APP35US
Page 18

In light of the above remarks, an early and favorable response is earnestly requested.

Respectfully submitted,

/Stephen J. Driscoll/
Registration No. 37,564
Attorney for Applicant
Synnestvedt & Lechner LLP
1101 Market Street, Suite 2600
Philadelphia, PA 19107-2950
Telephone: (215) 923-4466
Facsimile: (215) 923-2189

SJD/dl

S:\C\COMCAST\Patents\P33368-J USA\PTO\response to 10-5-07 OA.doc